Uson

# White Paper
# FDA 21 CFR Part 11 for Medical Device Applications

## Uson's Sprint$^{mD}$ and Optima$^{vT}$ leak testers are designed to help medical device manufacturers comply with 21 CFR Part 11

Author:
Chetan Desai, Director of Technology at Uson
+1-281-671-2034
chetan.desai@uson.com

### Introduction

Part 11 in Title 21 of the Code of Federal Regulations includes the US Federal guidelines for storing and protecting electronic records and applying electronic signatures.

The intent of these guidelines is to ensure that applicable electronic records are reliable, authentic, and maintained with high integrity. This white paper describes features and functionality of the Sprint$^{mD}$ and Optima $^{vT}$ software that enables customers to meet the guidelines of 21 CFR Part 11.

This document examines each section of 21 CFR Part 11 and provides a detailed analysis of features implemented in software to support the computer system validation process.





Uson L.P. | 8640 N. Eldridge Parkway | Houston, TX 77041 USA
Phone: +1-281-671-2000 | Uson.com

## Background

Rule 21 CFR Part 11 was originally issued in 1997 by the United States Food and Drug Administration (FDA) as a response to industry demands. This regulation presented criteria for accepting electronic records, electronic signatures, and handwritten signatures. With this regulation, titled Rule 21 CFR Part 11, electronic records can be equivalent to paper records and handwritten signatures. FDA issued two guidance documents in 2001 and 2003 to further explain and clarify the regulation's scope and application.

## Why CFR Part 11 Is Important

In 1997, the amount of digitized data and digital record-keeping capabilities was very different than it is today. In the two decades since 21 CFR Part 11 was issued, the ruling has become even more relevant and important to the medical device industry. Today, the medical device industry benefits from increased automation and digitization to achieve their compliance objectives. Electronic records are not only more cost effective, but they also ensure data integrity. Additionally, electronic records support a shorter approval process and provide faster, more productive access to documentation.

## Scope of 21 CFR Part 11

The scope of FDA 21 CFR Part 11 pertains to electronic records, electronic signatures, audit trail, and computer systems. 21 CFR Part 11 applies to companies that comply with the Food, Drug, and Cosmetic Act and the Public Health Service Act and includes current Good Manufacturing Practice (cGMP). To understand the importance of Part 11 today, it is necessary to revisit the original meaning of the regulation.

## Closed Versus Open System

A closed system is an environment where system access is controlled by the company using it. The company can confirm the identity of all users prior to providing access to the electronic record system and only electronic signatures are required. A closed system is defined as an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

An open system is an environment where system access is not controlled by the company using it. The company cannot confirm the identity of all users prior to providing access to the electronic record system. In addition to electronic signatures, digital signatures are also required to verify the identity of the person signing the document. An open system is an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.


*Sprint mD Leak & Flow Tester*


*Optima vT Leak & Flow Tester*



Uson L.P. | 8640 N. Eldridge Parkway | Houston, TX 77041 USA
Phone: +1-281-671-2000 | Uson.com

## Electronic Signatures

Officially, an electronic signature is "a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature". Simplified, that means an electronic signature is any electronic approval of a quality or production record.

An electronic signature must be comprised of two parts to ensure it is unique and ties to a specific person. 21 CFR Part 11 suggests the two distinct identification components should be an identification code and password:

> "…electronic signatures to be unique to one individual" 11.100(a) by "employing at least two distinct identification components such as an identification code and password" 11.100(a)(1) and "maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password." 11.300(a)

The first part of an electronic signature – the identification code – may be well known, such as a username or email address. Within a company, the user I.D. must be unique to a specific person that permits "limiting system access to authorized individuals" (21 CFR Part 11.10 (d)).

21 CFR part 11 also presents requirements for password management and protection. It requires that the combined identification code and password are unique and not duplicated within the same organization, and that measures are taken to ensure passwords are checked or changed periodically, to prevent password impairment, and that loss procedures are in place to deauthorize passwords in the event they are lost, stolen, or otherwise compromised. (11.300)

Furthermore, the system must "use authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand" 11.10(g). Also, the FDA advises administrative control to change signatures by stating "…use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals" 11.200(a)(3).

The Sprint$^{mD}$ and Optima$^{vT}$ are designed to support this requirement by forcing a user to set his or her individual password after initial login. Once passwords are set, they are persisted to permanent storage.

Once configured by authorized user (administrator), the Sprint$^{mD}$ an Optima$^{vT}$ software requires a username and password combination to edit programs, settings, and other controlled pages in the software. The Sprint$^{mD}$ and Optima$^{vT}$ uniquely identifies authorized individuals and restricts access to certain operations per the individual's assigned role (operator, supervisor, or administrator).



Uson L.P. | 8640 N. Eldridge Parkway | Houston, TX 77041 USA
Phone: +1-281-671-2000 | Uson.com

To ensure that passwords are frequently changed, the FDA also requires that "…password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging)" 11.300 (b).

Both the Sprint$^{mD}$ and Optima$^{vT}$ can be configured to have passwords expire and timeout logins as necessary in addition to providing optional administrative best practices to enforce password content requirements and enforce password policies, such as minimum password length or retry count, etc.

## Audit Trail

User-independent, time-stamped audit trails are also required to comply with 21 CFR part 11. An audit trail of an electronic record system provides evidence as to the generation of electronic records, when electronic records were signed electronically, who signed the electronic records, and related history. All electronic records and electronic signatures need to be date and time stamped and include an audit trail.

Per 21 CFR part 11.10(h), use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction. When configured, the unique serial number of the tester can be saved to the "Audit Log" record.

When the Sprint$^{mD}$ or Optima$^{vT}$ are configured to store data on a local hard drive, the results are saved in the Audit Log. Initial configuration is done at the Uson factory, and only administrators can make changes to the configuration. The number of results saved in the Audit Log is limited only by storage space. Both the Sprint$^{mD}$ and the Optima$^{vT}$ can be configured to store data, including the Audit Log results, on a network drive. When data is saved on a network drive, the end user is responsible for ensuring access to this file is restricted to authorized personnel. Both testers also allow data to be exported to a USB memory drive for inspection and review.

Validation is an important consideration when it comes to 21 CFR Part 11. For example, it is important to be able to accurately reproduce all system data in a format that is both readable by electronic systems as well as humans [11.10(b)]. The Sprint$^{mD}$ and Optima$^{vT}$ save audit trail data in human-readable text format.

Both the Sprint$^{mD}$ and Optima$^{vT}$ are available with enhanced security features, such as user authentication through passwords and roles, customizable access authorization, and the ability to log and monitor changes to test parameters. The tester uniquely identifies authorized individuals and restricts access to certain operations per the individual's assigned role—operator, supervisor, or administrator. This is important, because 21 CFR Part 11 requires electronic records contain 1) the printed name of the signer, 2) the data and time when the signature was executed, and 3) the intent, such as review, approval, responsibility, or authorship, associated with the signature. Both testers support all three requirements.



Uson L.P. | 8640 N. Eldridge Parkway | Houston, TX 77041 USA
Phone: +1-281-671-2000 | Uson.com

## Operational Checks

21 CFR 11.10(f) includes guidelines to ensure that electronic records created are authentic. It contains language to ensure procedures are followed in the correct order, and that changes to records—creation, deletion, or modification—follow the permitted sequence of steps and events. Also, the system needs to have a way to enforce this.

Once the Sprint$^{mD}$ or Optima$^{vT}$ tester is configured by an administrator, the tester program execution sequence is strictly controlled. This program can only be modified by an authorized supervisor.

The Sprint$^{mD}$ an Optima$^{vT}$ both allow the user to configure timing (timing depends on the type of part or component being leak tested), but the actual sequence of steps—such as those shown in the screen above, from Auto Zero to Vent—is controlled by the software and cannot be changed. This is how the testers maintain operational order. The specific step sequence is dictated by the type of test. Different types of tests will have different step sequences.

**Record Protection**

Procedures are required to ensure that data is retained throughout the stated lifetime of the data, per 21 CFR 11.10(c). The records need to be protected for accuracy and easily retrievable for the duration of their retention period.

The Sprint$^{mD}$ and Optima$^{vT}$ have a range of options available for storing data. There is no direct access to the data generated by the tester, other than through the interface. Data cannot be modified within the leak tester. Audit trail data can be exported to a network drive or USB media from the local drive, and data can be directly stored on a network location—both shared and secured network drives).

## Conclusion

US FDA guidelines for storing and protecting electronic records—known as 21 CFR Part 11—has been in place for more than 20 years. However, due to advancements in technology and innovation, combined with the sheer volume of data being generated, the regulation has never been as relevant as it is today for medical device manufacturers. The Sprint$^{mD}$ and Optima$^{vT}$ make it possible for medical device manufacturers to move new products into manufacturing quickly, and both testers support the instrument qualification and operational qualification (IQ/OQ) processes with greater efficiency.

The Sprint$^{mD}$ and Optima$^{vT}$ software was designed specifically to help end users comply with 21 CFR Part 11. The instrument contains all the essential features required to support the compliance process, such as electronic signatures and an audit trail. Compliance with 21 CFR Part 11 is a shared responsibility, with specific areas only the end user can implement and enforce. These areas are identified in this document, but additional actions may be required that are not in the scope of this document.



Uson L.P. | 8640 N. Eldridge Parkway | Houston, TX 77041 USA
Phone: +1-281-671-2000 | Uson.com

## Relevant Links

**FDA 21 CFR Part 11 (USA)**
https://www.fda.gov/downloads/RegulatoryInformation/Guidances/ucm125125.pdf

**Medicines and Healthcare Regulatory Agency (UK)**
https://www.gov.uk/government/organisations/medicines-and-healthcare-products-regulatory-agency

**Current Good Manufacturing Practice (CGMP) Regulations**
https://www.fda.gov/Drugs/DevelopmentApprovalProcess/Manufacturing/ucm090016.htm



Uson L.P. | 8640 N. Eldridge Parkway | Houston, TX 77041 USA
Phone: +1-281-671-2000 | Uson.com

## Appendix

The chart on the following pages can be used as a tool for assessing a leak tester to support your compliance requirements.

| 11.10 Controls for Closed Systems | | | |
|---|---|---|---|
| Section | Regulation | Interpretation | Y/N |
| 11.10(a) | Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. | Has the tester been validated for functionality during the development of the product? Is testing performed on each unit to ensure it meets strict performance guidelines? | |
| 11.10(b) | The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records. | Can the tester be configured (access restricted) to store data on a local hard drive, with results saved in an "Audit Log"? Are the number of results limited only by storage space?<br>Can the tester be configured to store data on a network drive, with results saved in the "Audit Log" on the network drive? (End user is responsible for ensuring access to this file is restricted to authorized personnel.)<br>Can data be exported to a USB memory drive for inspection, review, and copying? | |
| 11.10(c) | Protection of records to enable their accurate and ready retrieval throughout the records retention period. | Is the number of results that can be stored is limited only by storage space? Can data be exported to a USB memory drive for inspection, review, and copying? | |
| 11.10(d) | Limiting system access to authorized individuals. | Can the tester uniquely identify authorized individuals and restrict access to certain operations per the individual's assigned role (operator, supervisor, or administrator)? | |
| 11.10(e) | Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | Are modifications to the program recorded in the "Audit Trail" with date and time record, along with the identification of operator that performed the action? | |
| 11.10(f) | Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate. | Once configured, can the tester program execution sequence be strictly controlled and only modified by an authorized supervisor? | |



Uson L.P. | 8640 N. Eldridge Parkway | Houston, TX 77041 USA
Phone: +1-281-671-2000 | Uson.com

| 11.10 Controls for Closed Systems | | | |
|---|---|---|---|
| Section | Regulation | Interpretation | Y/N |
| 11.10(g) | Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | Does the tester uniquely identify authorized individuals and restrict access to certain operations per the individual's assigned role (operator, supervisor, or administrator)? | |
| 11.10(h) | Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction | When configured, can the unique serial number of the tester be saved to the "Audit Log" record? | |
| 11.10(i) | Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks. | Are records of the employment history, experience, and training of employees be verified and made available during an on-site audit? | |
| 11.10(j) | The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification. | N/A – It is the responsibility of the organization implementing electronic signatures to develop written policies which ensure that individuals responsible for signing documents understand that their electronic signature is as equally binding as their handwritten signature. | |
| 11.10(k) | Use of appropriate controls over systems documentation including: | — | |
| 11.10(k)(1) | Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. | N/A – Though documentation is provided by Uson for its testers, the storage and distribution of this material is responsibility of the organization that implements and uses the system. | |
| 11.10(k)(2) | Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation. | Do formal change management procedures and documents exist for all revisions? | |



Uson L.P. | 8640 N. Eldridge Parkway | Houston, TX 77041 USA
Phone: +1-281-671-2000 | Uson.com

| 11.50 Signature Manifestations | | | |
|---|---|---|---|
| Section | Regulation | Interpretation | Y/N |
| 11.50(a) | Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:<br><br>(1) The printed name of the signer;<br>(2) The date and time when the signature was executed; and<br>(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature. | Does the tester uniquely identify authorized individuals and restrict access to certain operations per the individual's assigned role (operator, supervisor, or administrator)? | |
| 11.50(b) | The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout). | Once persisted, is the password assigned to a specific role and no longer visible? Does the password field show asterisks on entry and record have a hash in the database? Can the password only be reset by an authorized supervisor? | |

| 11.70 Signature/Record Linking | | | |
|---|---|---|---|
| Section | Regulation | Interpretation | Y/N |
| 11.70(a) | Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means. | If electronic signatures are used to approved records, can the signatures be modified by ordinary means on the generating tester? | |



Uson L.P. | 8640 N. Eldridge Parkway | Houston, TX 77041 USA
Phone: +1-281-671-2000 | Uson.com

| 11.100 Electronic Signatures: General Requirements | | | |
|---|---|---|---|
| Section | Regulation | Interpretation | Y/N |
| 11.100(a) | Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else. | Can the leak tester uniquely identify authorized individuals? | |
| 11.100(b) | Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual. | N/A – It is the responsibility of the organization implementing the system to ensure compliance with this regulation. | |
| 11.100(c) | Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures. | N/A – It is the responsibility of the organization implementing the system to ensure compliance with this regulation. | |
| 11.100(c)(1) | The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857. | N/A – It is the responsibility of the organization implementing the system to ensure compliance with this regulation. | |
| 11.100(c)(2) | Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature. | N/A – It is the responsibility of the organization implementing the system to ensure compliance with this regulation. | |



Uson L.P. | 8640 N. Eldridge Parkway | Houston, TX 77041 USA
Phone: +1-281-671-2000 | Uson.com

| 11.200 Electronic Signature Components and Controls | | | |
|---|---|---|---|
| Section | Regulation | Interpretation | Y/N |
| 11.200(a) | Electronic signatures that are not based upon biometrics shall: | — | |
| 11.200(a)(1) | Employ at least two distinct identification components such as an identification code and password. | Can the leak tester uniquely identify authorized individuals using two distinct identification components—a user ID and password? | |
| 11.200(a)(1)(i) | When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. | Can the leak tester uniquely identify authorized individuals and restrict access to certain operations per the individual's assigned role (operator, supervisor, or administrator)? | |
| 11.200(a)(1)(ii) | When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. | Can the leak tester prevent unauthorized access to certain features based on the permissions assigned? | |
| 11.200(a)(2) | Be used only by their genuine owners; and | Once persisted, is the password assigned to a specific individual, and the password is no longer visible? | |
| 11.200(a)(3) | Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals. | Does the leak tester force a user to set their individual password after initial login? Are passwords set and confirmed after they are persisted? | |
| 11.200(b) | Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners. | N/A – Biometric devices are typically external to leak testers. | |

| 11.300 Controls for Identification Codes/Passwords | | | |
|---|---|---|---|
| Section | Regulation | Interpretation | Y/N |
| 11.300(a) | Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password. | Can the leak tester uniquely identify authorized individuals using two distinct identification components—a user ID and password? | |
| 11.300(b) | Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging). | Can the leak tester be configured to age passwords and timeout logins as necessary? | |
| 11.300(c) | Following loss management procedures to electronically de-authorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls. | N/A – Token generating devices are typically external to leak testers. | |
| 11.300(d) | Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management. | Does the leak tester permit password policies such as password aging and minimum length, etc.? | |
| 11.300(e) | Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner. | N/A – Token generating devices are typically external to leak testers. | |

Uson
for good measure

At Uson, we work closely with our customers to understand their unique and changing needs. We combine this insight with the knowledge of cutting-edge technologies to predict the future needs of our customers and their industries. With the largest installed base of leak testers in the medical device industry, we build leak testers and accessories to the highest standards, as demanded by the world's leading manufacturers. This unrivaled experience and expertise is complemented by global sales and support.

Visit us at **www.uson.com** for more information.



Uson L.P. | 8640 N. Eldridge Parkway | Houston, TX 77041 USA
Phone: +1-281-671-2000 | Uson.com